

Azure Firewall

- ✓ Create Rg-italy
- ✓ Create FirewallVnet with two subnets 1.default(subnet),
2. firewall (firewall subnet) Dedicated subnet
- ✓ Next Create SpokeVm with SpokeVnet and its subnet.

Home > Network foundation | Virtual networks

Create virtual network

Add a subnet

Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add several subnets to this virtual network.

Basics Security IP addresses Tags

+ Add a subnet

Subnet purpose: Azure Firewall

Name: AzureFirewallSubnet

IPv4

Include an IPv4 address space:

IPv4 address range: 10.0.0.0/16
10.0.0.0 - 10.0.255.255

Starting address: 10.0.1.0

Size: /26 (64 addresses)

Subnet address range: 10.0.1.0 - 10.0.1.63

IPv6

Include an IPv6 address space: This virtual network has no IPv6 address ranges.

Private subnet

Add Cancel

Previous Next Review

Create virtual network

Validation passed

Basics Security IP addresses Tags Review + create

Subscription: Azure subscription 1

Resource Group: Ufirewall-rg

Name: Ufirewall-Vnet

Region: Italy North

Security

Azure Bastion: Disabled

Azure Firewall: Disabled

Azure DDoS Network Protection: Disabled

IP addresses

Address space: 10.0.0.0/16 (65,536 addresses)

Subnet: Usubnet (10.0.0.0/24) (256 addresses)

Subnet: AzureFirewallSubnet (10.0.1.0/26) (64 addresses)

Previous Next Create Download a template for automation

✓ Now lets Create Firewall

Create a firewall ...

Subscription * Azure subscription 1

Resource group * Ufirewall-rg [Create new](#)

Instance details

Name * Ufirewall01

Region * Italy North

Availability zone ⓘ None

Firewall SKU

Basic
 Standard
 Premium

Create a firewall ...

Firewall management

Use a Firewall Policy to manage this firewall
 Use Firewall rules (classic) to manage this firewall

Choose a virtual network

Create new
 Use existing

Virtual network Ufirewall-Vnet (Ufirewall-rg)

Public IP address * (New) Ufirewall-pip [Add new](#)

Firewall Management NIC

Firewall Management NIC separates Firewall management traffic from customer traffic. A dedicated subnet is required with its own associated public IP address that will be used exclusively by the Azure platform and can't be used for any other purpose.

Enable Firewall Management NIC



ⓘ Critical Firewall features such as Forced Tunneling and Packet Capture require management NIC to be enabled.

[Previous](#) | [Next : Tags >](#) | [Download a template for automation](#)



✓ **Next create SpokeVm in same region and give its subnet.**

Create a virtual machine



Help me create a low cost VM

Validation passed



Help me create a low cost VM

Help me create a VM optimized for high availability

Subscription	Azure subscription 1
Resource group	(new) Uspoke-rg
Virtual machine name	Uspoke-vm
Region	Italy North
Availability options	No infrastructure redundancy required
Zone options	Self-selected zone
Security type	Standard
Image	Windows Server 2025 Datacenter - Gen2
VM architecture	x64
Size	Standard D2ads v5 (2 vcpus, 8 GiB memory)
Enable Hibernation	No
Username	azureuser
Public inbound ports	RDP
Already have a Windows license?	No
Azure Spot	No

Networking

Virtual network	vnet-italynorth
Subnet	snet-italynorth-1
Public IP	(new) Uspoke-vm-ip
Accelerated networking	On
Place this virtual machine behind an existing load balancing solution?	No
Delete public IP and NIC when VM is deleted	Disabled



Uspoke-vm



Help me copy this VM in any region

Manage this VM with Azure CLI

Virtual machine

Search



Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Connect

Networking

Settings

Availability + scale

Security

⚠️ Uspoke-vm virtual machine agent status is not ready. Troubleshoot the issue →

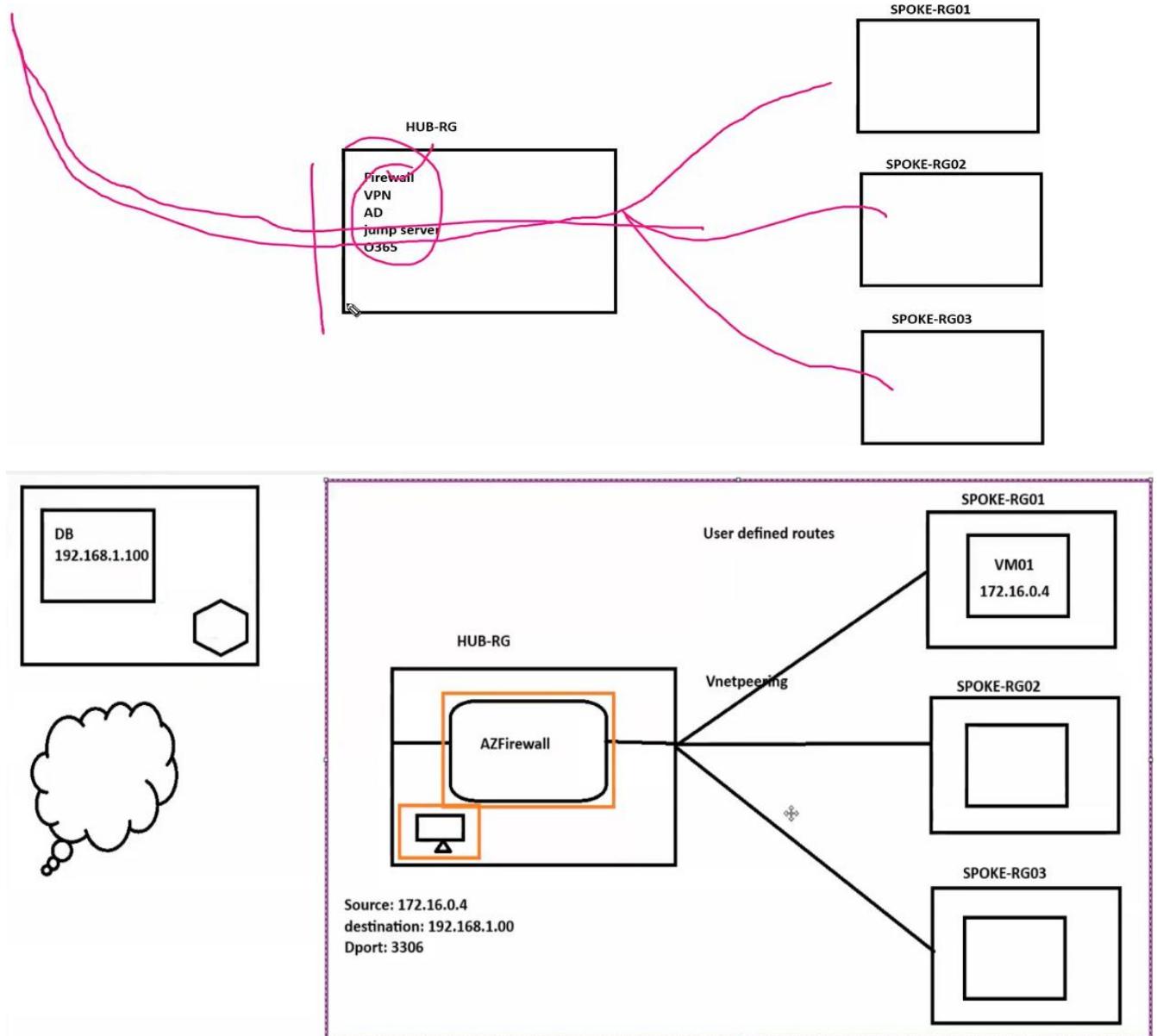
Help me copy this VM in any region

Connect ▾ Start ▾ Restart ▾ Stop ▾ Hibernate ▾ Capture ▾ Delete ▾ Refresh ▾ Scale ▾ Open in mobile ▾ Feedback

^ Essentials

Resource group (move)	: Uspoke-rg	Operating system	: Windows
Status	: Running	Size	: Standard D2ads v5 (2 vcpus, 8 GiB memory)
Location	: Italy North	Primary NIC public IP	: 172.213.227.14 1 associated public IPs
Subscription (move)	: Azure subscription 1	Virtual network/subnet	: vnet-italynorth/snet-italynorth-1
Subscription ID	: 5d75b66d-66bf-44e0-8d7e-7e61e4b043d7	DNS name	: Not configured
		Health state	: -
		Time created	: 13/02/2026, 10:24 UTC

HUB & Spoke Architecture



- ✓ Machines behind the firewall, by default there will be denied rule we can't access the machines
- ✓ From public even though machines have public Ip once the machine is behind the firewall by default traffic will be blocked.
- ✓ For now, we created Firewall and Spokevm (windows)
- ✓ Let's log into spokevm(pip)
- ✓ Next Lets config Vnet peering from **firewallVnet & SpokeVnet**

✓ We see two diff Vnet for firewall and spoke below

Network foundation | Virtual networks

Virtual network

Name ↑	Resource Group	Location
<input checked="" type="checkbox"/> Ufirewall-Vnet	Ufirewall-rg	Italy North
<input type="checkbox"/> VFIREWALLRG1	VFIREWALLRG1	South Africa North
<input type="checkbox"/> vnet-canadacentral	VSPOKE-RG1	Canada Central
<input type="checkbox"/> BH-rg	BH-rg	Central India
<input checked="" type="checkbox"/> vnet-italynorth	Uspoke-rg	Italy North

✓ Choose any Vnet for peering

Ufirewall-Vnet | Peerings

Peerings

Name ↑	Peerings
	Showing all 0 items

Add peering

Remote virtual network summary

Peering link name *	firewall-to-spoke
I know my resource ID ⓘ	<input type="checkbox"/>
Subscription *	Azure subscription 1
Virtual network *	vnet-italynorth (Uspoke-rg)

Remote virtual network peering settings

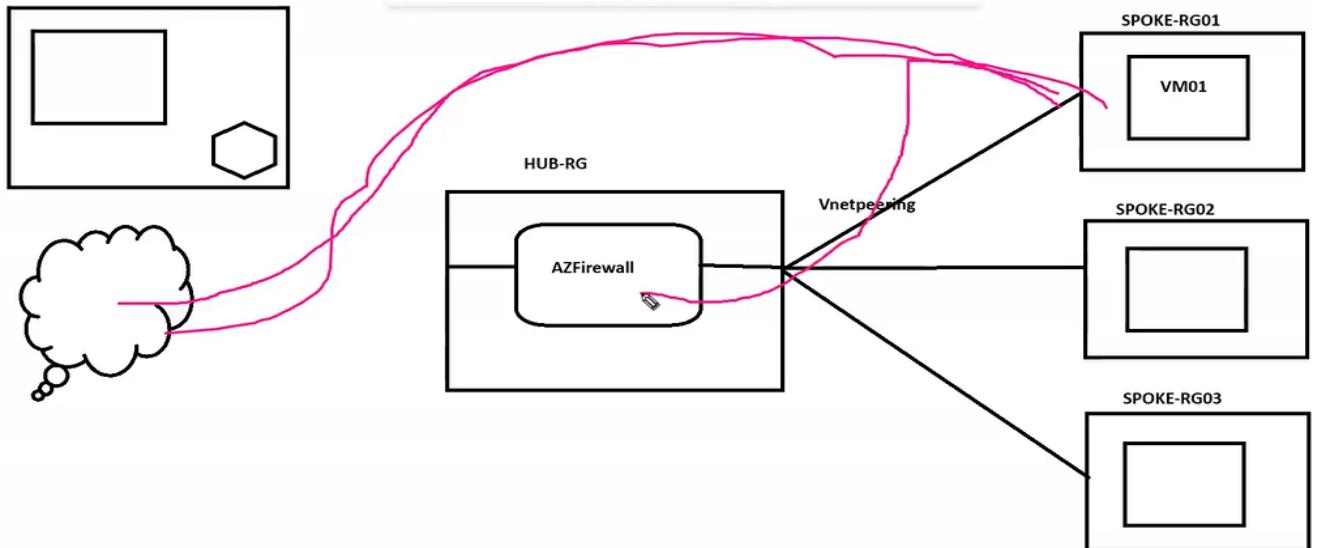
Allow 'vnet-italynorth' to access 'Ufirewall-Vnet' ⓘ	<input checked="" type="checkbox"/>
Allow 'vnet-italynorth' to receive forwarded traffic from 'Ufirewall-Vnet' ⓘ	<input type="checkbox"/>
Allow gateway or route server in 'vnet-italynorth' to forward traffic to 'Ufirewall-Vnet' ⓘ	<input type="checkbox"/>
Enable 'vnet-italynorth' to use 'Ufirewall-Vnet's remote gateway or route server ⓘ	<input type="checkbox"/>

Local virtual network summary

Peering link name *	spoke-to-firewall
---------------------	-------------------

Add Cancel

- ✓ After Vnet peering we can still connect to spokeVm bcz the traffic is going through outside and connecting to spokeVm.



- ✓ Let's Redirect traffic to firewall
- ✓ For that use should right **Route Table (User Defined Routes)**
- ✓ Search for Route Tables and click on Create

Create Route Table

[Basics](#) [Tags](#) [Review + create](#)

Select the subscription to manage deployed resources and costs. Use resource groups like told me to manage all your resources.

Subscription *	<input type="text" value="Azure subscription 1"/>
Resource group *	<input type="text" value="Uspoke-rg"/> Create new

Instance details

Name *	<input type="text" value="UspokeRT"/>
Propagate gateway routes *	<input type="radio"/> Yes <input type="radio"/> No
Region *	<input type="text" value="(Europe) Italy North"/>

✓ Below click on Add and add route

UspokeRT | Routes

Route table

Search

Add Refresh Give feedback

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

Configuration

Routes

Subnets

Search routes

Name ↑↓ Address

No results.

Home > RouteTableDeployment-1770984473171 | Overview > UspokeRT

UspokeRT | Routes

Route table

Search

Add Refresh Give feedback

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

Configuration

Routes

Subnets

Properties

Locks

Monitoring

Search routes

Name ↑↓ Address prefix

No results.

Add route

UspokeRT

Route name * To_Firewall

Destination type * IP Addresses

Destination IP addresses/CIDR ranges * 0.0.0.0/0

Next hop type * Virtual appliance

Next hop address * 10.0.1.4

Add

✓ **0.0.0.0/0 is Any above. Copy below Firewall Private Ip Below**

Ufirewall01

Firewall

Search

Migrate to firewall policy Delete Lock Change SKU

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

Show the latest IDPS hits for this firewall

How to protect my firewall against failures

For advanced security protection of your network, you can easily upgrade to Azure Firewall Premium

Resource group (move)	SKU
Ufirewall-rg	Standard(change)
Location	Subnet
Italy North	AzureFirewallSubnet
Subscription (move)	Public IP
Azure subscription 1	Ufi Copied
Subscription ID	Private IP
5d75b66d-66bf-44e0-8d7e-7e61e4b043d7	10.0.1.4

- ✓ Now from SpokeVm whatever the traffic it should hit firewall first
- Now Next Once We Write the Route rule it should be attached to Subnet

Home > RouteTableDeployment-1770984473171 | Overview > UspokeRT

UspokeRT | Subnets

Route table

Search

+ Associate

Subnets

No results.

Associate subnet

UspokeRT

Virtual network ⓘ

vnet-italynorth (Uspoke-rg)

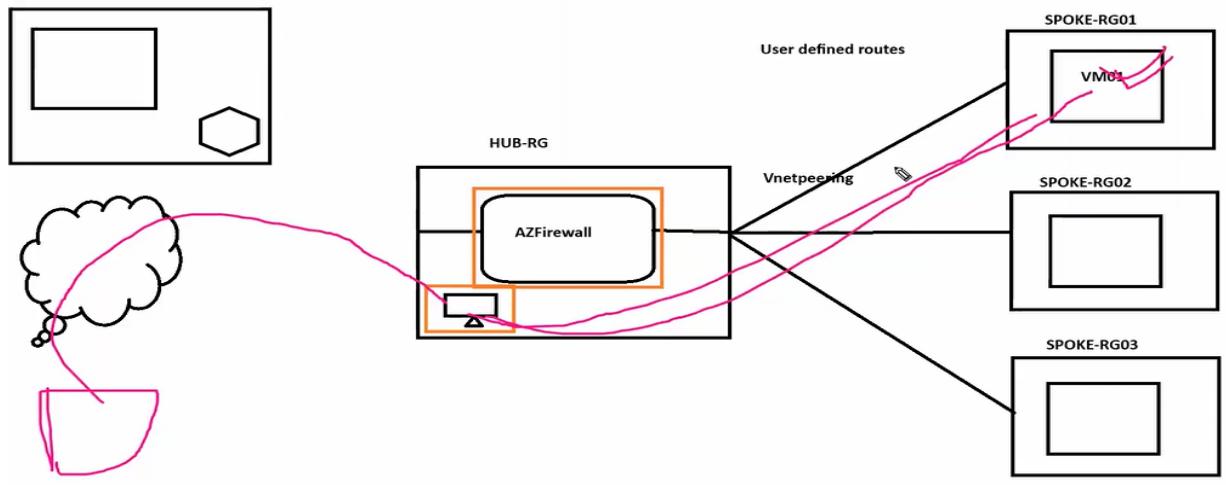
Subnet * ⓘ

snet-italynorth-1

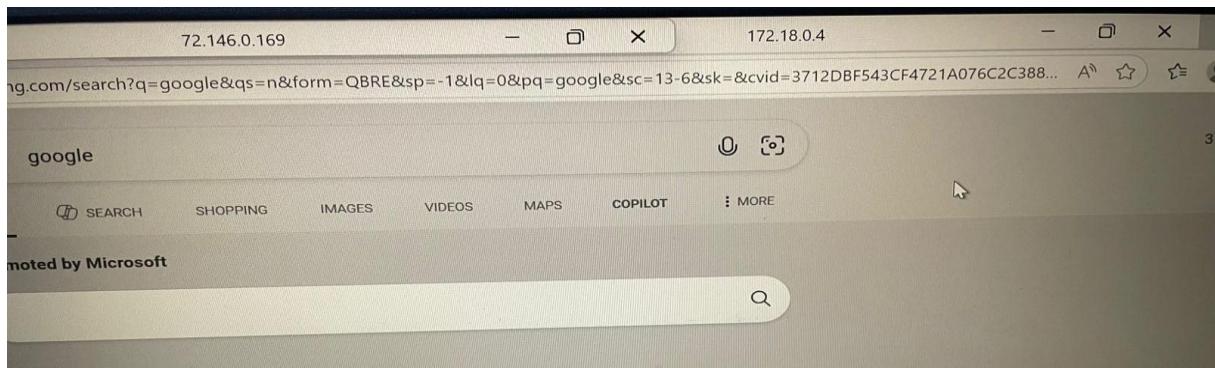
- ✓ We have defined Routing, so the traffic coming from inside it should use Azure Firewall only, the traffic will flow from firewall only.
- ✓ After adding the rules to subnet automatically SpokeVM which is logged in earlier it will disconnect, Bcz traffic Diverted from firewall.



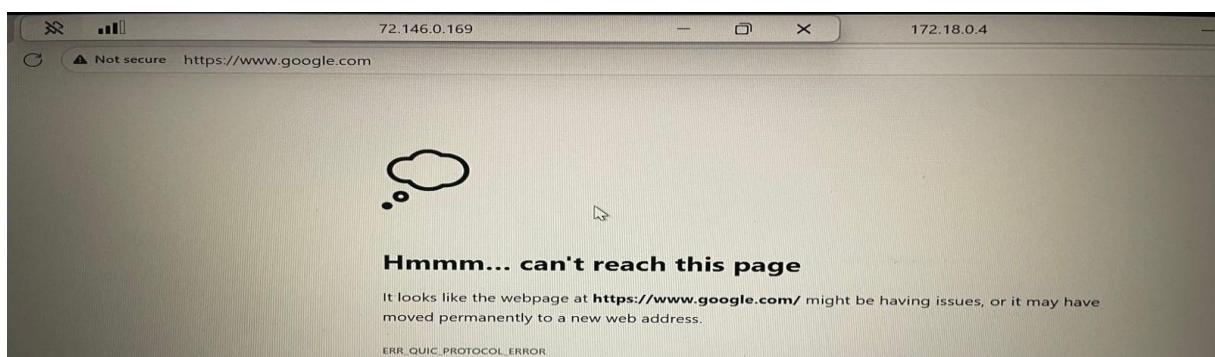
- Next create another VM using subnet in FirewallVnet.
- This VM just to know what's happening in SpokeVM.
- To access this from my **LAPTOP** → **VM** → **SPOKEVM**



- ✓ Let's create **VM (windows)** on **HUB-RG(FirewallVnet)**
- ✓ Now Connect to this VM using **PublicIP(72.146.0.169)** on RDC
- ✓ After connecting to VM, open RDC in it and **Connect to SpokeVM internally** by using **SpokeVM PrivateIP(172.18.0.4)**



- ✓ We can't access anything bcz internet is not allowed and rules not match on firewall and this is behind the firewall.



❖ Let's talk about Rules (follow below steps)

Network security | Azure Firewall Policies ...  Identify policies imp

Preview

Search Filter for any field... Subscription equals all

+ Create Manage view Refresh Export to CSV

Overview

Firewall Manager

Azure Firewalls

Azure Firewall Policies

WAF + DDoS

Secure your resources

Create an Azure Firewall Policy ...

Basics DNS Settings TLS Inspection Rules IDPS Threat intelligence Tags Review + create

Define network and application level rules for traffic filtering across multiple Azure Firewall instances in Secured Virtual Hub

Project details

Subscription * Azure subscription 1

Resource group * Ufirewall-rg Create new

Policy details

Name * defaultpolicy

Region * Italy North

Info Parent policy must be in the same region as child policy. Firewall policy can be associated with Firewalls across regions regardless of their region.

Your new policy will inherit all rule collections from the selected parent policy below. Rule collections inherited from the parent policy will be merged with the new policy.

Policy tier Standard Basic Premium

Parent policy None

Review + create Previous Next : DNS Settings > Download a template for automation

Create an Azure Firewall Policy ...

Validation passed

Basics DNS Settings TLS inspection Rules IDPS Threat intelligence Tags **Review + create**

Summary

Subscription	Azure subscription 1
Resource group	Ufirewall-rg
Name	defaultpolicy
Region	Italy North
Policy tier	Standard

Rules

Parent policy None

Rule collections

RULE COLLECTION TYPE	
No results	

 Microsoft.FirewallPolicy-20260213212221 | Overview ...

Deployment

Search X << Delete Cancel Redeploy Download Refresh

Overview

Inputs Outputs Template

Your deployment is complete

Deployment name : Microsoft.FirewallPolicy-20260213212221
Subscription : Azure subscription 1
Resource group : Ufirewall-rg

> Deployment details
▽ Next steps

Go to resource

- ✓ **Created Name(`defaultpolicy`) but we didn't added rules in it, let's do that.**

 **defaultpolicy** 

Firewall Policy

Search ◇

Resource visualizer

> Management

▽ Rules

Rule collections

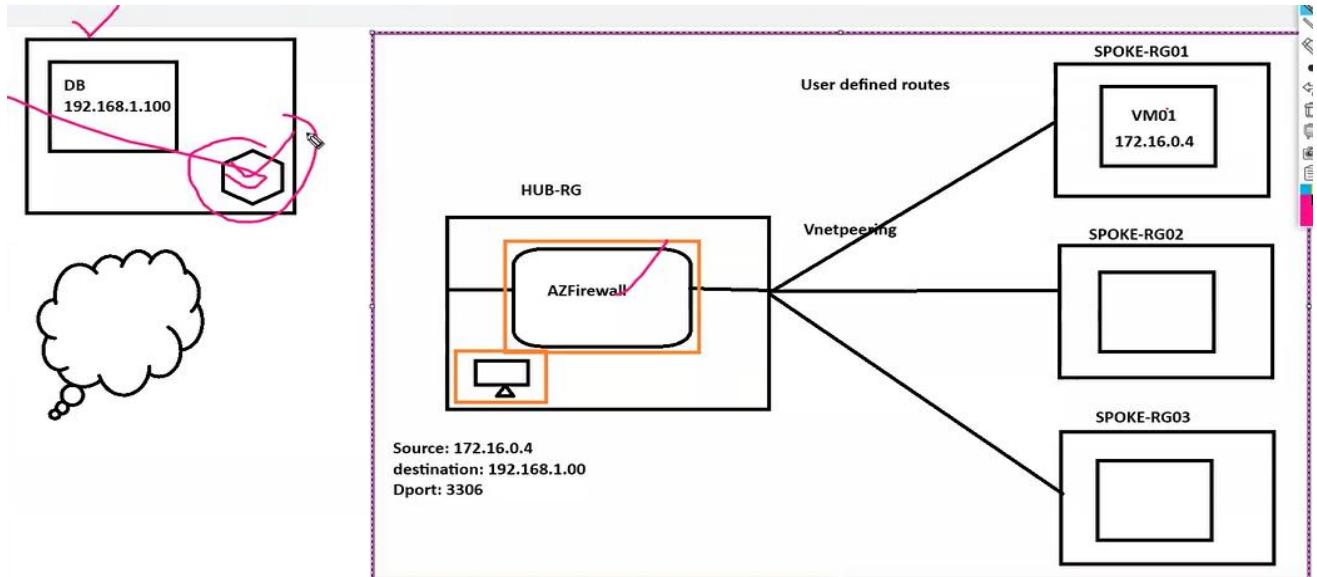
DNAT rules

Network rules

Application rules

- ✓ **Network rule** if we want to allow IP to IP then we use it.
- ✓ We don't use domain names here
 - Below you can see example which we used in lab.

- ✓ App & DB in different datacentres and they both have firewalls and both should config firewall rules then only we can access both.



Home > Microsoft.FirewallPolicy-21 defaultpolicy | Network Firewall Policy

Add a rule collection

Name *	Allow_DB
Rule collection type *	Network
Priority *	100
Rule collection action	Allow
Rule collection group *	DefaultNetworkRuleCollectionGroup

Rules

Name *	Source type	Source	Protocol *	Destination Ports *	Destination Type *	Destination *
Allow_DB	IP Address	*	0 selected	3306	IP Address	192.168.1.100
	IP Address	*, 192.168.10.1, 192...	0 selected	80,8000-9000	IP Address	*10.0.0.1,10.1.0.0/1...

❖ Application rules

defaultpolicy | Application rules ★ ...

Firewall Policy

Rules

- Rule collections
- DNAT rules
- Network rules
- Application rules**

Rules are shown in the order of execution below. Network rules take precedence over rule collection group priority and rule collection priority.

Search to filter items...

Rule Collection P...↑ ↓ Rule collection n... Rule name

No application rule collections found

Home > Microsoft.FirewallPolicy-20260213: Add a rule collection

defaultpolicy | Application Firewall Policy

Name * Allow_Internet

Rule collection type * Application

Priority * 100

Rule collection action Allow

Rule collection group * DefaultApplicationRuleCollectionGroup

Rules

Name *	Source type	Source	Protocol *	TLS inspection	Destination Type *	Destination *
Allow_google	IP Address	*	http,https	<input checked="" type="checkbox"/> TLS inspection	FQDN	*.google.com
Allow_yahoo	IP Address	*	http,https	<input checked="" type="checkbox"/> TLS inspection	FQDN	*.yahoo.com

- ✓ Associate this defaultpolicy to your Firewall
- ✓ Go to firewall → Migrate to firewall policy → Attach an existing firewall policy below

Home > Network security | Azure Firewalls

Ufirewall01 Firewall

How can my firewall stop that threat

Search Overview Activity log Access control (IAM)

Migrate to firewall policy Delete

Migrate to firewall policy
Attach an existing firewall policy

Home > Network security | Azure Firewalls Select an Azure Firewall Policy

Ufirewall01 Firewall Manager

Selected Firewall Policy will override the current policy and rules on the firewall

Firewall Policy	Inherits From	Firewall Policy Tier	Subscription	Resource Group
<input checked="" type="checkbox"/> defaultpolicy		Standard	Azure subscription 1	Ufirewall-rg

- ✓ Select above policy and save.

❖ DNAT rules

- ✓ Below I want to connect from internet to backend machine.
- ✓ Like from My laptop to directly Backend machine, but we can't connect bcz the machine is behind the firewall.
- ✓ But in this case, we can cannot by use Firewall Public IP
- ✓ Outside traffic hits to Firewall Public IP from that traffic will go to Backend machine, here Backend Private IP masked by firewall.
- ✓ Firewall PublicIP (172.213.217.109) → Backend SpokeVM PrivateIP (172.18.0.4)
- ✓ Same with ports 50000 → 3389
- ✓ Translating with Public → Private and from Port → Port for Security to Machine, we are just Mapping with one to one.
- ✓ We can choose servers; on those we can add this Mapping at in emergency situations then access backend machines.

The screenshot shows the 'Add a rule collection' page in the Azure portal. The rule collection type is set to 'DNAT'. The 'DNAT rules' section is selected in the left sidebar. A table below lists a single rule: Source * (asterisk), Protocol * (TCP), Destination Ports * (50000), Destination (Firewall IP) (172.213.217.109), Translated type * (IP Address), Translated address or (172.18.0.4), and Translated port * (3389).

Example Below:

Protocol *	Destination Ports *	Destination (Firewall IP)	Translated type *	Translated address or	Translated port *
TCP	50000	20.172.146.62	IP Address	172.16.0.4	3389
	50001	20.172.146.62		172.16.0.5	3389
	50002	20.172.146.62		172.16.0.6	3389

⊕ There is another option DNATTING → we connect with Private IPs only by using VPS, we can login into the azure infrastructure to one of the gem servers from there we are going to connect.

Copy firewallPublicIP:50000

By this we can connect to Backend SpokeVM

